UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

# FSIS NOTICE	64-15	9/29/15

USE OF FSIS GOVERNMENT-FURNISHED EQUIPMENT

I. PURPOSE

This notice provides FSIS Federal and non-Federal employees (e.g., contractors) with instructions regarding the acceptable and unacceptable use of FSIS government furnished equipment (GFE) (e.g., telecommunications resources, computers, laptops, and smartphones) and Government-issued e-mail addresses. This notice also announces the need for some employees to complete an FSIS mobile device agreement.

II. USE OF GFE's FOR TELECOMMUNICATIONS

A. DR 3300-001 explains that USDA employees are allowed the limited personal use of telecommunications resources (e.g., telephones, facsimile, electronic messaging, computer equipment, and the Internet) in the workplace on an occasional basis, provided that the use involves minimal expense to the Government and does not interfere with official business. According to DR 3300-001, employees are normally to use telecommunications resources for personal use during the employees' personal time. USDA employees are to exercise common sense and good judgement in the personal use of telecommunications resources. Official Government business is to always take precedence over the personal use of telecommunications resources. Agencies and staff offices may supplement DR 3300-001 as required to clarify internal operating procedures.

B. FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets out the Agency's policy regarding the use of GFEs. This notice is specifically restricting the use of FSIS e-mail addresses (e.g., John.Public@fsis.usda.gov) to only government related business. Employees are not to use their FSIS email address for any other purpose such as online shopping, setting other e-mail accounts (e.g., Yahoo, Google), or subscriptions to non-government publications. The Agency is aware that such activities pose an increased risk to Agency, Departmental, and Federal infrastructure, data, and resources. Attachment 1 provides of list of currently prohibited activities related to use of GFE's.

C. Employees are to be aware that the Office of Chief Information Officer (OCIO) routinely monitors and controls all computer access points (e.g., Universal Serial Bus, FireWire®, infrared, Bluetooth, wireless Ethernet). There is no right to privacy on U.S. government systems, e-mail, or equipment.

III. FSIS EMPLOYEE RESPONSIBILITIES

A. Employees are to complete annual Federal and USDA mandated training (e.g., Security Awareness and Privacy training).

B. Employees are to use the USDA/FSIS Local Area Network (LAN) or VPN for Internet browsing using GFE including use during the employee's personal time (e.g., weekends (if the employee has access to the work site), before and after work, lunchtime, or during scheduled break periods). No off-Agency network Internet access, except when necessary to connect to the USDA/FSIS network, is permitted.

C. Employees are not to access the USDA-FSIS network or process FSIS sensitive-but-unclassified information on any computer or device that is not FSIS GFE.

D. Employees are to ensure that all removable media devices, such as CDs, DVDs, removable hard drives, and thumb drives containing sensitive but unclassified information, including Personally identifiable information (PII), are encrypted at the Federal Information Processing Standards (FIPS)140-2 standard and use an OCIO-approved device.

IV. FSIS MOBILE DEVICE AGREEMENT

FSIS employees and contract employees who use mobile devices (e.g., smart phones and tablets) provided by FSIS for work purposes are to review the rules of behavior and sign the FSIS Mobile Acceptable Use and Rules of Behavior Agreement (Level 2 eAuthentication is needed to access this information and form on InsideFSIS). After completing the agreement, employees are to submit it to their supervisor. Supervisors are to maintain signed copies of the agreements for all their employees that use mobile devices.

V. QUESTIONS

Refer questions regarding this notice to the FSIS Security Operations Center at: OCIOSecurityOperationsCenter@fsis.usda.gov.

Assistant Administrator
Office of Policy and Program Development

Attachment 1

PROHIBITED USES OF GFE's

FSIS explicitly prohibits the use of GFE (including government-issued e-mail addresses) for:

1. Accessing or processing pornographic material, gaming or gambling content;

2. Accessing non-work-related streaming internet radio or media;

3. Giving out personal information about another person outside of work, including home addresses and phone numbers, unless approved by the supervisor for emergency purposes;

4. Installing software (including shareware, freeware and toolbars);

NOTE: Only an FSIS Service Desk technician or authorized Office of Chief Information Office information technology (OCIO IT) specialist may install Technical Change Control Board-approved hardware and software to Agency computers, unless otherwise directed by OCIO;

5. Accessing file-sharing services (e.g., Dropbox, Google Drive, One Drive);

6. Sharing FSIS network accounts. Accounts are not to be shared and are to be used solely on USDA network systems for authorized business purpose;

7. Connecting Non-FSIS computers to the FSIS network, either directly or through a Virtual Private Network (VPN) connection, except for authorized use of approved Secure Socket Layer (SSL) VPN by OCIO;

8. Using the network for commercial or for-profit purposes;

9. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the network;

10. Using the network to disrupt the use of the network by others. Hardware or software cannot be destroyed, modified, or abused in any way;

11. Maliciously using the network to develop programs that harass other users or infiltrate a computer or computing system or damage the software components of a computer or computing system;

12. Sending hate mail, chain letters, harassment, discriminatory remarks or content, or other inappropriate behaviors;

13. Downloading, copying, otherwise duplicating, or distributing copyrighted materials without the specific written permission of the copyright owner;

14. Using the network for any unlawful purpose;

15. Using profanity, obscenity, racist terms, or other language or content that may be offensive to another user; and

16. Leaving FSIS computers in an operational state while unattended. Unattended computer are to require Ctrl+Alt+Del and a password or smart card to become operational.